



Securing Tomorrow's Missions Today.



Before You Rewrite It: A Fixed-Fee Modernization Assessment and Increment Plan for One Legacy Application

Application Modernization: an evidence-scored decision, a target architecture and a slice-by-slice plan for one legacy application, with reauthorization planned in from the start

AvalonTechServices.com

contact@AvalonTechServices.com

Executive Summary	2
Why Legacy Applications Stall	3
Why Rewrites Fail	3
The Mandates and the Calendar	4
What the Assessment Does	5
The Disposition Decision	6
The Increment Plan	6
Deliverables	7
Where the Engagement Stops	7
Evidence the ISSM Can Use	8
How an Engagement Runs	9
What the Agency Provides	9
What Is Not Included	10
How Avalon Staffs It	10
Pricing and How to Buy	11
Illustration: One Application, Eight Weeks	12
Labor Loading	12
What the Engagement Costs	13
What the Agency Brings to the Readout	13
Common Pitfalls	14
Conclusion and Next Step	14
Appendices	15
Appendix A: Glossary	15
Appendix B: Illustration Assumptions	15
Appendix C: References	16

Executive Summary

Most agencies have at least one application everyone agrees must be modernized and nobody wants to touch. It runs a mission process, it sits on an operating system or database that is out of vendor support or close to it, two people understand its business rules, and every change takes a contract modification. The usual response is a large rewrite proposal, which stalls because nobody can say what the application actually does, what depends on it, or whether a rewrite is even the right answer.

The calendar is forcing the question. SQL Server 2016 reached end of extended support on July 14, 2026, and Windows Server 2016 follows on January 12, 2027. An application built on either fails NIST SP 800-53 control SA-22 (Unsupported System Components) by definition, and the ISSO will raise it at the next reauthorization. For civilian agencies, CISA Binding Operational Directive 26-04 (June 10, 2026) adds risk-based remediation clocks for known exploited vulnerabilities, and a component that can no longer be patched cannot meet them.

This paper is for the people who own that application: the program manager or system owner who funds it, the CIO who sets the target platforms, the ISSM or ISSO who carries the findings, and the COR who buys the work. It describes Avalon Technology Services' Application Modernization service, which starts with one engagement:

- **A fixed-fee modernization assessment for one named application.** One unclassified, non-mainframe application, about eight weeks. Discovery and assessment in the agency's own repository, an evidence-scored disposition (retain through retire), a target-state architecture, and a strangler-fig increment plan with reauthorization checkpoints built into the roadmap. The market band for a single-application assessment is \$50K to \$100K firm fixed price; Avalon's anchor for this work is \$50K to \$150K depending on scope.
- **A conditional execution follow-on.** Incremental modernization of the same application, priced separately against the roadmap, with a market band of \$500K to \$2.5M.

Section 9 works through the effort model. The base case is 464 hours over eight weeks at a blended \$165 to \$195 an hour: \$76.6K to \$90.5K, with a \$84K planning fee, well under the \$350,000 simplified acquisition threshold.

The service engineers the decision, the design and the plan. The authorization decision remains the government's. Avalon does not issue or guarantee an ATO, does not act as the independent assessor of a system it modernizes, and does not certify compliance.

Why Legacy Applications Stall

The phrases below come up in almost every conversation about a federal legacy application. Each one is a reason to modernize; none of them says how.

What the program says	What it usually means
"It takes six months and a contract mod to change a field."	Business rules live in code nobody has mapped, so every change is a research project
"There are two people left who understand it, and one retires next year."	The real system documentation is in two people's heads
"Our ISSO says it won't survive reauthorization."	Unsupported components (SA-22) or unpatchable findings sit on the POA&M with no closure path
"We're paying extended support just to keep it on life support."	The run cost is growing and nobody has priced the alternative
"We can't hire for that platform anymore."	The skills risk is now larger than the technical risk
"We tried to modernize it before and the project failed."	A big-bang rewrite with frozen requirements and late reauthorization

Why Rewrites Fail

- **The default answer is chosen first.** "Move it to the cloud" or "rewrite it" is decided before anyone has scored the application, so a system that should be retained, replatformed or retired gets a rewrite budget.
- **Business rules are not recovered.** Code is translated, often now with AI assistance, without first capturing what the old system actually does. The result is a new legacy system in a newer language.
- **Interfaces are discovered late.** Upstream feeds, downstream consumers, batch jobs and shared databases surface during cutover, not during planning.

- **Reauthorization is an afterthought.** A modernization is a significant change under NIST SP 800-37, which triggers reassessment. When that is not on the roadmap, a finished system waits months for its authorization.
- **Decommissioning is skipped.** The new system goes live and the old one keeps running, so the agency pays both run costs.

The Mandates and the Calendar

Driver	What it says	What it means for this engagement
NIST SP 800-53 Rev. 5, SA-22	Replace components when the vendor no longer supports them, or provide approved alternative sources of support	The control legacy applications fail by definition; the assessment names every unsupported component
Windows Server 2016 and SQL Server 2016	SQL Server 2016 support ended July 14, 2026; Windows Server 2016 support ends January 12, 2027	The cleanest, most datable trigger; the roadmap dates every end-of-support event in the stack
CISA BOD 26-04 (Jun 10, 2026)	Risk-based remediation clocks for known exploited vulnerabilities, from three days with forensic triage to 14 days, 60 days or the next upgrade; replaced BOD 22-01 and BOD 19-02	A component that cannot be patched cannot meet the clock; civilian agencies only
NIST SP 800-37 Rev. 2	Seven RMF steps, starting with Prepare; a significant change triggers reassessment	Reauthorization checkpoints go into the roadmap, not after cutover
OMB M-26-14 (May 2026)	A risk-based logging model; replaced M-21-31	The target design states what the modernized application logs and where

Driver	What it says	What it means for this engagement
OMB M-22-09 and CISA Zero Trust Maturity Model 2.0	Civilian zero trust strategy; five pillars including applications and workloads	Legacy applications are often the blocker to the agency's zero trust plan
FedRAMP Consolidated Rules (Jun 25, 2026)	Cloud offerings are "FedRAMP Certified" in classes A through D; certification covers the provider's offering only	Constrains the target platform; the agency still authorizes its own system
Section 508 and the 21st Century IDEA Act (2018)	Accessibility (the 2017 refresh incorporates WCAG 2.0 AA) and modern public-facing digital services	Public-facing modernizations carry both into the target design
DoD CSRMC (announced Sep 24, 2025)	A new risk management construct; RMF, DoDI 8510.01 and eMASS remain in use	DoD business systems still reauthorize through existing RMF records

Two notes on funding and assurance. The Technology Modernization Fund was extended through fiscal year 2026; agencies should confirm its current status before planning around it. And OMB M-26-05 (January 23, 2026) rescinded M-22-18 and M-23-16: NIST SP 800-218 (the Secure Software Development Framework) is guidance, and an SBOM is a contract term the agency may choose for the modernized application, not a mandate.

What the Assessment Does

The assessment covers one named application and goes deep. Portfolio-wide disposition across many systems is Avalon's separate IT Modernization service; this engagement starts where that one stops, or stands alone when the agency already knows which application hurts. It works in the agency's own repository and tooling, using open-source analysis tools such as SonarQube, Konveyor and OpenRewrite, and installs nothing of Avalon's.

Step	Activities
Discovery and assessment	Application inventory; static analysis for size, language mix, complexity, dead code and embedded business rules; SME interviews; infrastructure and licensing inventory
Dependency and interface map	Every upstream feed, downstream consumer, batch job and shared database, named and counted
Run-cost baseline	Extended-support fees, specialist hours, hosting and change lead time, from agency-supplied figures
Security posture review	The current SSP and POA&M read against the stack: unsupported components, unpatchable findings and logging gaps
Disposition	An evidence-scored decision with the scoring workbook the agency can defend internally
Target state and increment plan	Architecture, service decomposition, data approach, identity integration and a sequenced roadmap with reauthorization checkpoints

The Disposition Decision

Every assessment ends in one explicit decision from the standard set: retain, rehost, replatform, refactor, rearchitect, rebuild, or replace and retire. Each option is scored against four criteria: mission criticality, technical health, cost, and compliance exposure. The evidence for each score is written down, so the program can defend the decision to its CIO and budget office. "Retain" is a legitimate outcome. If the evidence says the application should stay where it is with a narrow fix, the assessment says so.

The Increment Plan

When the decision is to change the application, the plan uses the strangler-fig pattern: new services stand up alongside the legacy system, traffic moves to them one slice at a time, and legacy functions retire as each slice proves out. Each slice has a functional-parity baseline, automated regression tests that capture legacy behavior before anything changes, and rollback criteria. APIs let downstream consumers move on their

own schedule. The roadmap marks where each slice is a significant change under the RMF, so the ISSO and the assessor are scheduled, not surprised.

Deliverables

Deliverable	Format
Assessment and Disposition Report	PDF report with an XLSX scoring workbook
Target-State Architecture Package	Architecture document with editable draw.io and SVG diagrams
Modernization Roadmap: slices, funding phasing and reauthorization checkpoints	PDF with editable source
Component inventory, data flows and boundary diagrams in SSP-consumable form	Files the SSP author can use directly

Where the Engagement Stops

The assessment stops at the roadmap. Lift-and-shift with no code change is Avalon's separate Cloud Migration & Development service; landing zones belong to Cloud Architecture & Engineering; the delivery toolchain belongs to CI/CD Pipelines and DevSecOps. Writing the SSP and facilitating the ATO are separate workstreams, priced separately. Enterprise data cleanup beyond what the application's migration needs, and operations after cutover, are out of scope.

Evidence the ISSM Can Use

Control	What the assessment and follow-on address
SA-22	Unsupported system components: every one named, dated and assigned a disposition
SI-2, RA-5	Flaw remediation and vulnerability scanning on a stack that can be patched and scanned
CM-2, CM-8	Current baselines and a component inventory the SSP can cite
SC-8, SC-13	Modern cryptography in transit and at rest in the target design
AC-2, IA-2	Integration with enterprise identity and multifactor authentication
AU-2, AU-6	Logging designed to the agency's M-26-14 decisions
CP family	A recoverable target architecture with tested restore paths

The accurate way to state the value is narrow. A follow-on built from this roadmap eliminates the unsupported components underlying the findings it names, produces the system documentation, component inventory and data flows required for the SSP update, and positions the system for reassessment against the agency's 800-53 baseline. Where the application is the blocker, it removes the primary technical obstacles to the agency's zero trust implementation plan.

Accurate	Not accurate
Names every unsupported component and its end-of-support date	Achieves compliance
Produces SSP-ready inventory and data flows	Delivers an ATO
Plans reauthorization checkpoints into the roadmap	Speeds an ATO by a set percentage
An input to the ISSM, the assessor and the AO	Guarantees assessment success

How an Engagement Runs

Phase	Timing	What happens
0: Kickoff and access	2–4 weeks, in parallel	Accounts, repository and environment access, CAC or PIV where required; dependencies dated in writing
1: Discovery and assessment	4–8 weeks (base: 5)	Static analysis, SME interviews, interface map, run-cost baseline, SSP and POA&M review
2: Disposition, architecture and roadmap	3–6 weeks (base: 3)	Disposition scoring, target state, increment plan, readout; the natural contract break point
3–5: Execution (separate, conditional)	Months, scope-dependent	Strangler-fig slices, data migration rehearsals, cutover, decommissioning and knowledge transfer

A single mid-size, non-mainframe application typically runs six to twelve months end to end. The assessment is Phases 1 and 2 only, bought as a standalone firm-fixed-price task.

What the Agency Provides

- Account, network and repository access issued at award. CAC, PIV and network access can take 30 to 90 days at some components, so it is a dated government-furnished dependency in the statement of work.
- Four to eight hours a week from the system SMEs who hold the undocumented business rules.
- Source code, existing documentation, the current SSP and POA&M, and the agency's run-cost figures.
- ISSO or ISSM participation at the roadmap checkpoint.
- A COR with authority to make decisions within days, not weeks. Agency-caused delays move the schedule day for day.

What Is Not Included

Included	Separate work
Assessment, disposition and roadmap for one application	Portfolio disposition across many systems
Target-state architecture	Landing zone construction
Increment plan	Execution sprints, unless bought as the follow-on
SSP-consumable inventory and data flows	Writing the SSP or the authorization package
Agency-owned tools and repositories	Tool licensing or resale
Unclassified, non-mainframe applications	Mainframe, classified or cleared environments

How Avalon Staffs It

Avalon takes one engagement at a time, works business hours, and works on unclassified applications only. Avalon's founder serves as engagement lead and security and compliance specialist, with one named, certified solutions architect hired or subcontracted for the engagement. A legacy-platform SME is subcontracted only when the stack requires one. Avalon has no past federal engagements under this service. FAR 15.305 says an offeror without a record of past performance may not be evaluated favorably or unfavorably on that factor; what protects the program is a named team, a fixed price and a bounded scope. Avalon never serves as the independent assessor of a system it modernized.

Requirement	How it is handled
Solutions architect	Named personnel whose certifications and investigation level match the agency's requirements, listed in the proposal
Legacy-platform SME	Named in the proposal when the stack requires one; priced as a separate line
Privileged access on DoD systems	Personnel holding the DoD 8140 qualification the program requires, as a condition of the engagement
Civilian access	Public Trust investigation at the tier the agency requires
Platform	Work happens in the agency's repository and tooling with access the agency provisions; Avalon hosts nothing
Insurance and contract vehicles	Any coverage the solicitation requires is a condition of award; Avalon does not hold a GSA Schedule or a governmentwide contract today

Pricing and How to Buy

Engagement	Market-norm range	Avalon
Single-application assessment and roadmap, about 8 weeks	\$50K–\$100K	Firm fixed price within \$50K–\$150K depending on scope; illustrative \$84K
Single mid-size application execution, non-mainframe	\$500K–\$2.5M	Conditional follow-on, firm fixed price by milestone, with named personnel
Portfolio or mainframe modernization	\$5M and up	Not offered

The assessment sits under the \$350,000 simplified acquisition threshold and can be bought as an open-market purchase. Purchases between the \$15,000 micro-purchase threshold and the SAT are generally set aside for small business when two or more

capable small businesses are expected to compete. Larger execution work can be subcontracted to Avalon by a prime. Avalon does not hold a GSA Schedule or a governmentwide contract today, and it does not resell hardware, software or licenses.

Prices are fixed against one named application with scope caps on code size and interfaces, and a dated dependency schedule. There is no savings-linked or performance-based fee.

Illustration: One Application, Eight Weeks

The figures below are a planning illustration for one representative unclassified application: a case management application with a public-facing portal, built on Java on an aging application server, Windows Server 2016 hosts, SQL Server 2016. The statement of work caps scope at about 300K lines of code, 15 named external interfaces and 1 primary database. They are not a quote and not a result from any engagement.

Labor Loading

Role	Share of a week	Base hours (8 weeks)
Engagement lead / solutions architect	1.00 FTE	320
Security and compliance specialist	0.20 FTE	64
Project manager	0.25 FTE	80
Total	1.45 FTE	464

The architect is full time through both phases and owns the disposition and the target design. The security and compliance share reads the SSP and POA&M, maps unsupported components and places the reauthorization checkpoints. The project manager runs the dependency schedule and the readout. One blended rate of \$165 to \$195 an hour applies to every role.

What the Engagement Costs

Scope	Hours	Rate-band range	Planning fee	Inside \$50K–\$100K
Short (7 weeks)	406	\$67.0K–\$79.2K	\$73K	Yes
Base (8 weeks)	464	\$76.6K–\$90.5K	\$84K	Yes
Long (10 weeks)	580	\$95.7K–\$113.1K	\$104K	No: cap scope or split

The base case is five weeks of discovery and three of disposition and roadmap: 464 hours, or \$76.6K to \$90.5K, with a \$84K planning fee at the midpoint. A seven-week case runs \$67.0K to \$79.2K. A ten-week case runs \$95.7K to \$113.1K; the top breaks the single-application market band while staying inside Avalon's \$50K to \$150K anchor, so the statement of work caps interfaces and code size, or splits the application, instead of growing the fee.

If the stack needs a legacy-platform SME, the plan adds one at half time for Phase 1: 100 hours, or \$16.5K to \$19.5K, bringing the base case to \$93.1K to \$110.0K. Every case sits far below the simplified acquisition threshold.

What the Agency Brings to the Readout

The effort model prices the assessment; it does not claim a saving. The run-cost baseline is built from the agency's own figures: extended-support fees, specialist hours at the agency's labor rate, the hours spent on compensating controls for open SA-22 findings, and change lead time. Those numbers, not a vendor estimate, are what the program office takes to its budget office.

Common Pitfalls

Pitfall	How to avoid it
"While you're in there" feature requests	A functional-parity baseline and change control for every slice
Data cleanup with no end	Agency responsibility or a separately priced option, written into the statement of work
Interfaces found at cutover	A named interface inventory during discovery
Reauthorization left off the roadmap	Checkpoints with the ISSO and assessor scheduled per slice
Access lead time slips silently	Access requested at award as a dated government-furnished dependency
Different rates across bundled line items	One labor-rate table per proposal
AI-assisted conversion without recovered business rules	Rules captured and verified by people before code is translated

Conclusion and Next Step

A legacy application is rarely stuck for lack of money. It is stuck because nobody can say what it does, what depends on it, or which kind of change it needs, and so every proposal to fix it reads as a gamble.

The natural first step is the fixed-fee modernization assessment: one named application, about eight weeks, under the simplified acquisition threshold, ending in an evidence-scored disposition, a target-state architecture and an increment plan with reauthorization checkpoints the ISSO can schedule. To discuss an application, contact Avalon Technology Services at contact@AvalonTechServices.com.

Appendices

Appendix A: Glossary

Disposition

The explicit decision for an application: retain, rehost, replatform, refactor, rearchitect, rebuild, or replace and retire.

Strangler-fig pattern

Modernizing by standing up new services beside the legacy system and moving functions over one slice at a time.

SA-22

NIST SP 800-53 control for unsupported system components.

Significant change

A change to a system that triggers reassessment under the RMF (NIST SP 800-37).

Functional-parity baseline

A written record of what the legacy application does, used to test each new slice.

Run-cost baseline

The agency's current annual cost to operate and support the application, built from its own figures.

KEV catalog

CISA's Known Exploited Vulnerabilities catalog, which drives remediation clocks under BOD 26-04.

Appendix B: Illustration Assumptions

All values are planning assumptions for one representative unclassified application. None is drawn from a specific agency, a real system or a completed engagement.

Assumption	Value	Basis
Application	One case management application with a public-facing portal	Planning assumption
Scope caps	About 300K lines, 15 interfaces, 1 database	Planning assumption
Loading	Architect 1.0, security 0.2, PM 0.25 FTE	KB delivery model; PM share assumed
Duration	Phase 1 five weeks, Phase 2 three weeks	Inside KB phase ranges
Rate	\$165–\$195 an hour, all roles	Category rate card
Price check	Base fee \$84K	Inside \$50K–\$100K and \$50K–\$150K; under the SAT

Appendix C: References

1. **National Institute of Standards and Technology**, *SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations*
<https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final>
2. **National Institute of Standards and Technology**, *SP 800-37 Rev. 2, Risk Management Framework for Information Systems and Organizations*
<https://csrc.nist.gov/pubs/sp/800/37/r2/final>
3. **National Institute of Standards and Technology**, *SP 800-218, Secure Software Development Framework (SSDF) Version 1.1*
<https://csrc.nist.gov/pubs/sp/800/218/final>
4. **National Institute of Standards and Technology**, *SP 800-207, Zero Trust Architecture*
<https://csrc.nist.gov/pubs/sp/800/207/final>
5. **Cybersecurity and Infrastructure Security Agency**, *Zero Trust Maturity Model, Version 2.0*
<https://www.cisa.gov/zero-trust-maturity-model>

6. **Cybersecurity and Infrastructure Security Agency**, *Known Exploited Vulnerabilities Catalog*
<https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
7. **Tenable**, *CISA BOD 26-04 FAQ: Vulnerability Remediation Impact, June 11, 2026*
<https://www.tenable.com/blog/cisa-bod-26-04-FAQ-vulnerability-remediation-impact>
8. **Office of Management and Budget**, *M-22-09, Moving the U.S. Government Toward Zero Trust Cybersecurity Principles, January 26, 2022*
<https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf>
9. **Office of Management and Budget**, *M-26-05, Adopting a Risk-based Approach to Software and Hardware Security, January 23, 2026*
<https://www.whitehouse.gov/wp-content/uploads/2026/01/M-26-05-Adopting-a-Risk-based-Approach-to-Software-and-Hardware-Security.pdf>
10. **Office of Management and Budget**, *M-26-14, Ensuring Effective and Efficient Agency Logging and Network Visibility to Defend Against Evolving Cyber Threats, May 2026*
<https://www.whitehouse.gov/wp-content/uploads/2026/05/M-26-14-Ensuring-Effective-and-Efficient-Agency-Logging-and-Network-Visibility-to-Defend-Against-Evolving-Cyber-Threats.pdf>
11. **Microsoft**, *Windows Server 2016 and SQL Server 2016 lifecycle*
<https://learn.microsoft.com/en-us/lifecycle/products/>
12. **FedRAMP**, *FedRAMP program and 2026 Consolidated Rules*
<https://www.fedramp.gov>
13. **U.S. Access Board**, *Section 508 Standards (ICT Final Rule)*
<https://www.access-board.gov/ict/>
14. **Akin Gump**, *Department of Defense Launches CSRMC, a New Cybersecurity Risk Management Construct*
<https://www.akingump.com/en/insights/alerts/department-of-defense-launches-csrmc-a-new-cybersecurity-risk-management-construct>
15. **Acquisition.gov**, *FAR 15.305, Proposal evaluation*
<https://www.acquisition.gov/far/15.305>
16. **Centre Law & Consulting**, *Inflation Updates to FAR Thresholds: What Changed on October 1, 2025*

<https://centrelawgroup.com/blog/inflation-updates-to-far-thresholds-what-changed-on-october-1-2025/>